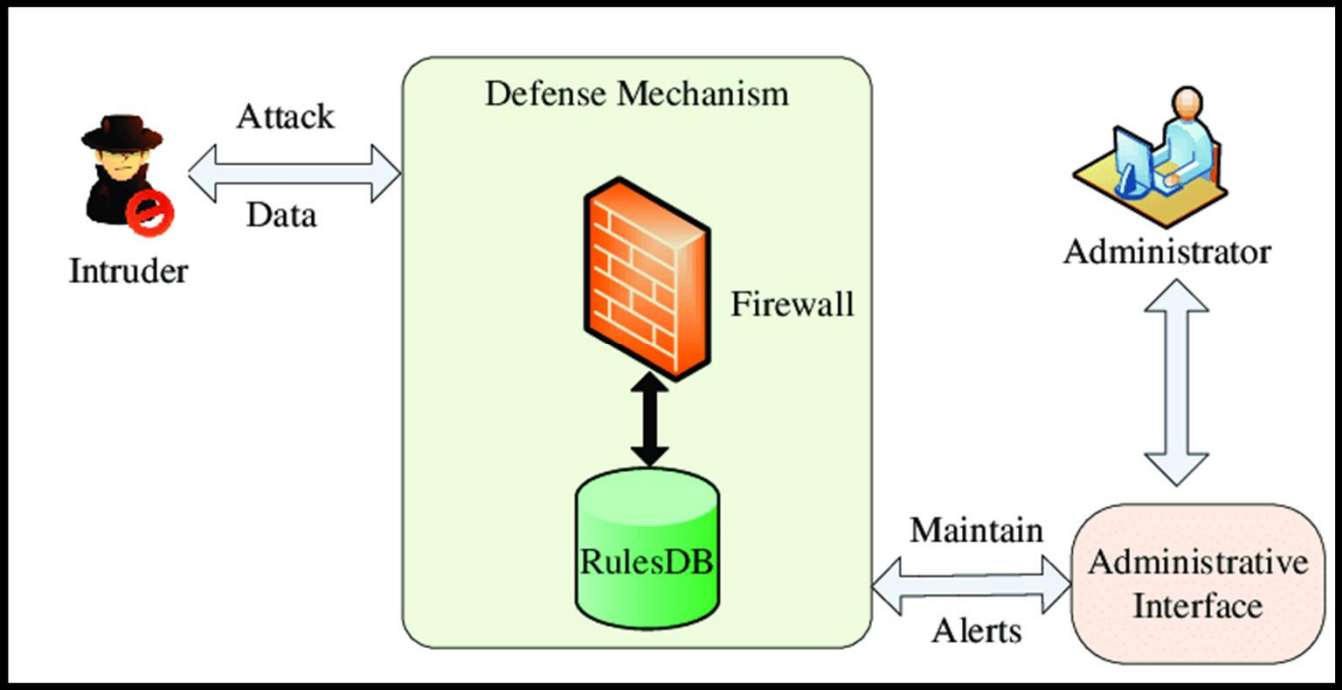
인공지능 보안
-10-

네트워크 보안

Network Intrusion Detection/Prevention

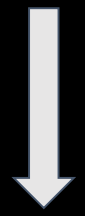
Network Intrusion Detection/Prevention



Defense Scenario I with firewall only.

Firewall

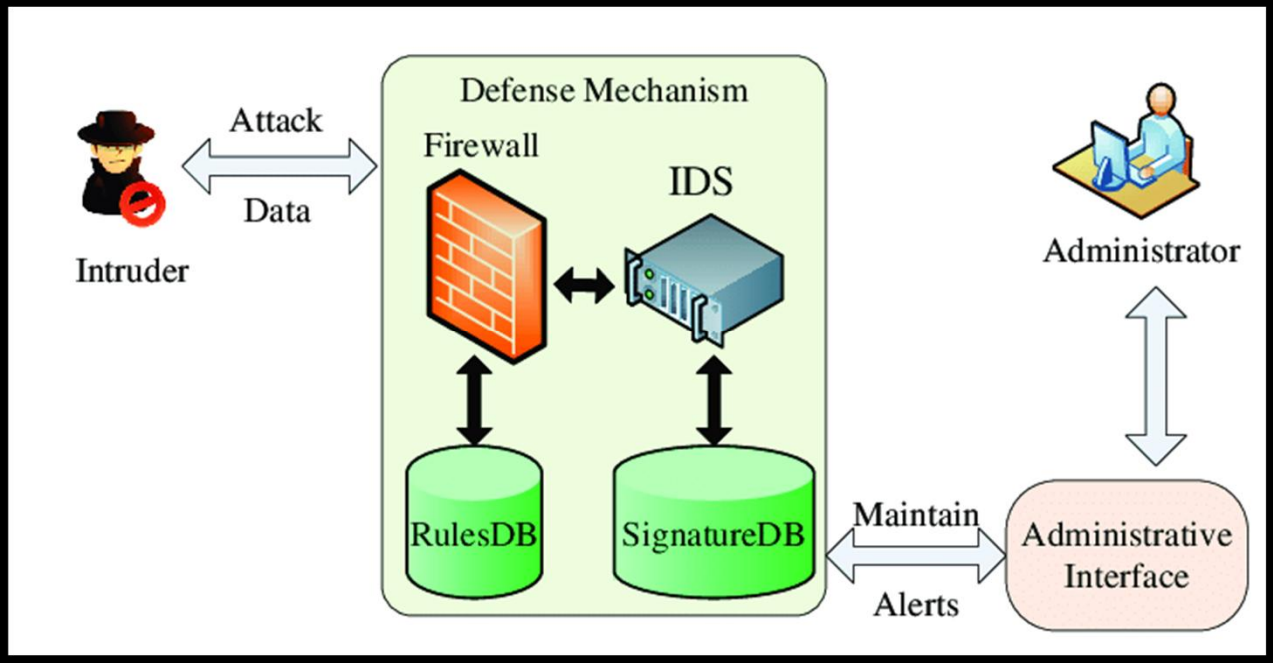
	Source Address	Souce Port	Dest Address	Dest Port	Action
1	Any	Any	192.168.1.0	>1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow
7	Any	Any	Any	Any	Deny



검색 방향

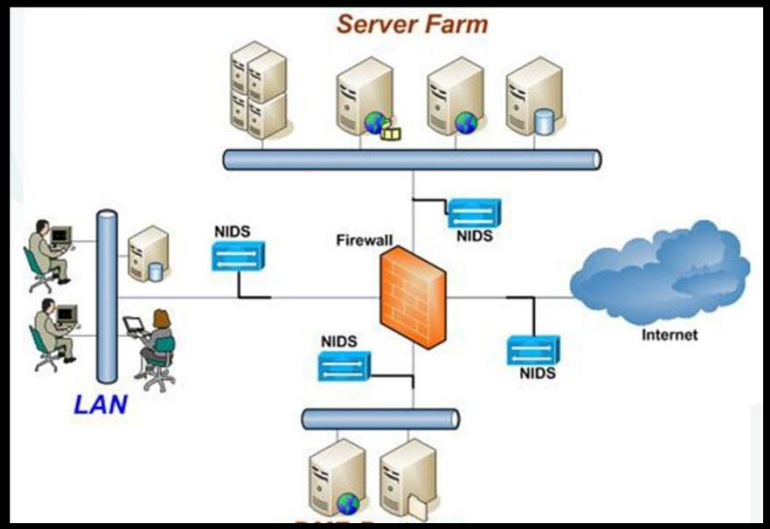
네트워크 트래픽을 모니터링하고 정의된 보안 규칙 집합을 기준으로 하여 특정 트래픽의 허용 또는 차단을 결정

Network Intrusion Detection/Prevention



Defense Scenario II with firewall and the Intrusion Detection System

NIDS/NIPS



각종 공격에 대한 특징(signature)을 분석하여 이것을 자동으로 감지할 수 있는 패턴형태로 만들어 놓고, 실시간으로 네트워크 패킷을 관찰하여 동일한 패턴이 발생하면 침입(Intrusion)을 알리는 오용탐지(Misuse Detection)가 주류

Snort

- 오픈 소스 침입탐지시스템
- 침입탐지시스템 중 가장 널리 사용
- 기능

  Packet Sniffer: 네트워크 상의 패킷을 sniffing하여 보여주는 기능
  Packet Logger: 모니터링한 패킷을 저장하고 로그에 남기는 기능
  IDS/IPS: 네트워크 트래픽을 분석해 공격을 탐지/차단하는 기능

(a) Header only (1.4%). Example:

```
alert tcp 88.76.243.5 67 -> 93.28.221.78 90 (msg: “knock knock”; sid: 9876;)
```

(b) Only Content (33%). Example:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (content: “Super blue
pills for super results!!!”; depth:42; sid: 5676;)
```

(c) Content and PCRE (65.5%). Example:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (uricontent:"/readme.eml";
content: “|2C|Read |FF 45| it”; distance:4; pcre: /a+bc\s{2}blah/R; sid: 435;)
```

(d) Only PCRE (0.1%). Example:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (pcre: “/^a+.?bc\s{2}
(Def)+|(Fed)+$/sm”; sid: 1098;)
```

PCRE

Perl Compatible Regular Expressions

이메일 - /^[0-9a-zA-Z]([-_₩.]?[0-9a-zA-Z])*@[0-9a-zA-Z]([-_₩.]?[0-9a-zA-Z])*₩.[a-zA-Z]{2,3}$/i

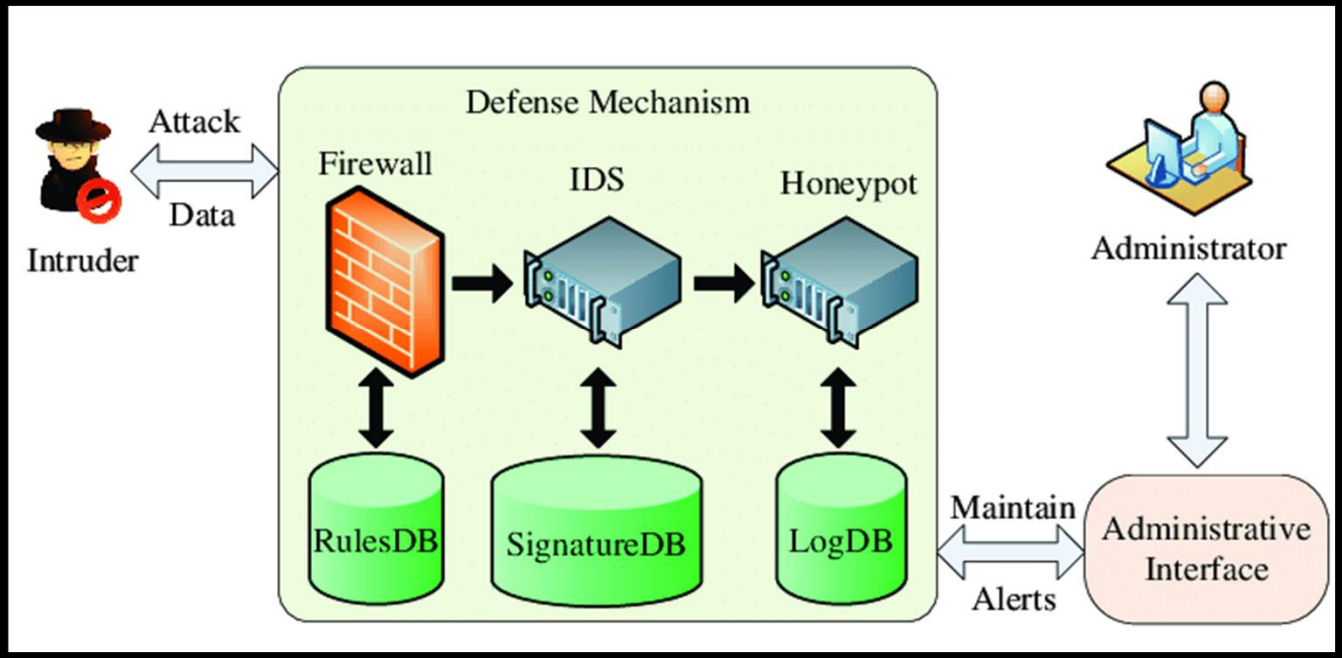
'시작을' 0~9 사이 숫자 or a-z A-Z 알바펫 아무거나로 시작하고 / 중간에 - _ . 같은 문자가 있을수도 있고 없을수도 있으며 /

그 후에 0~9 사이 숫자 or a-z A-Z 알바펫중 하나의 문자가 없거나 연달아 나올수 있으며 / @ 가 반드시 존재하고 /

0-9a-zA-Z 여기서 하나가 있고 / 중간에 - _ . 같은 문자가 있을수도 있고 없을수도 있으며 / 그 후에 0~9 사이 숫자 or a-z A-Z 알바펫중 하나의

문자가 없거나 연달아 나올수 있으며 / 반드시 . 이 존재하고 / [a-zA-Z] 의 문자가 2개나 3개가 존재 / 이 모든것은 대소문자 구분안함

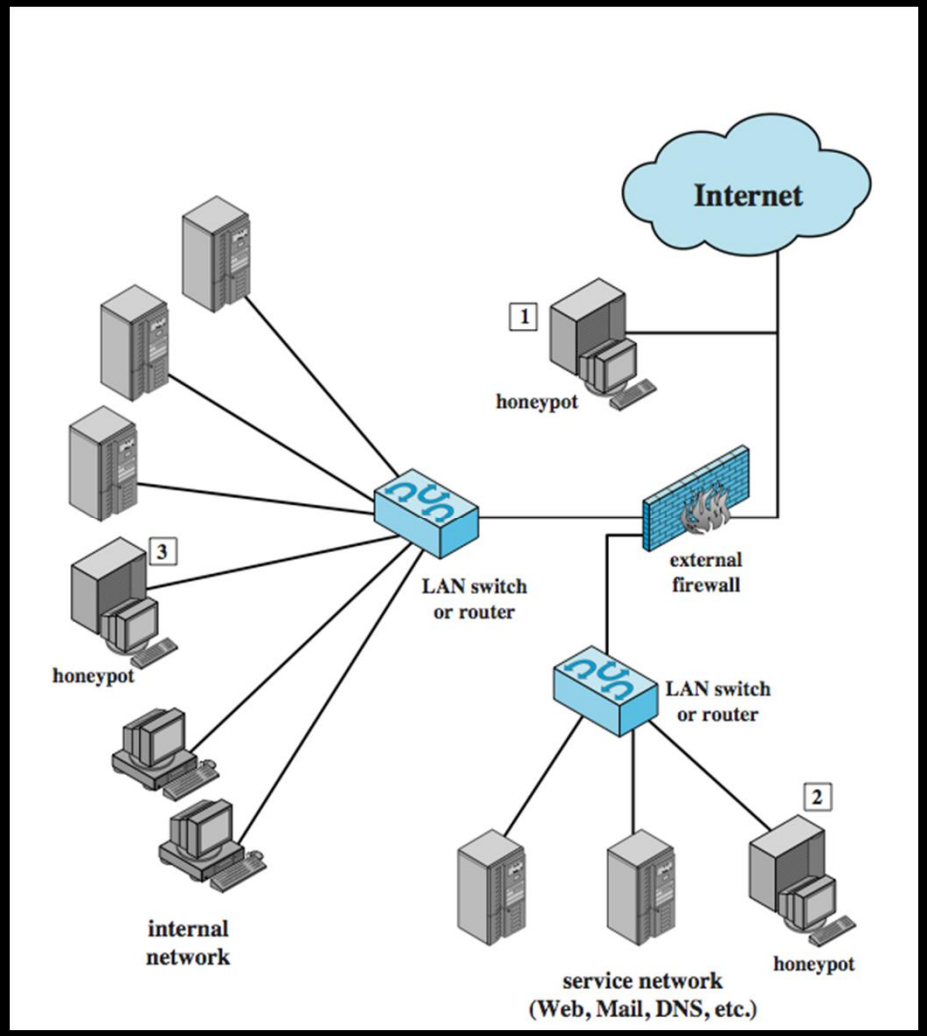
Network Intrusion Detection/Prevention



Defense Scenario III with firewall, IDS and honeypot.

Honeypot

- 비정상적인 접근을 탐지하기 위해 의도적으로 설치해 둔 미끼 시스템
- 조작된 정보로 채워지고 로깅 시스템 동작
- 공격자의 활동에 대한 정보 수집
- 처음에 단일 시스템이었으나 최근에는 전체 네트워크를 에뮬레이트



Q&A